State of Arizona
Department of Education

POLICY AND PROCEEDURE FOR

DATA COLLECTION, USE, AND ACCESS

Diane M. Douglas,
Superintendent of Public Instruction

Revision Date 12/30/2016

CONTENTS

INTRODUCTION AND OVERVIEW

The Arizona Department of Education (ADE) is charged with and takes very seriously the collection, management, and stewardship of education data records. As such, the ADE enforces policies concerning the use and sharing of data that preserves the privacy and rights of our students, educators, and system. ADE has created the following policies in order to assure consistent and accurate data that can be efficiently stored, managed, monitored, and reported while remaining securely encrypted to comply with state and federal requirements (FERPA).

Our priority is to ensure all Arizona children have the knowledge to determine their future, are prepared to achieve their goals and be successful citizens.

ARTICLE I. DATA COLLECTION

SECTION 1.01 POLICY

No ADE employee shall initiate a data collection without an approved data collection request, as outlined in this policy. A data collection initiated after the effective date of this policy that is not the result of an approved data collection request has no force or effect and the LEA receiving the request is under no obligation to respond.

Wherever and whenever possible, approved data collections shall be implemented via established data collection applications, to minimize confusion and maximize response rate. Decisions about how to implement data collections shall be made by the CDO and the ADE IT architecture team.

Pursuant to A.R.S. §15-1042(A), any changes to the student-level data elements to be collected by the Department must be submitted for review and approval by the Arizona Data Governance Commission.

The authority for an approved data collection expires and is revoked upon the expiration or repeal of the statute or regulation that requires the collection, or when the stated purpose has been achieved. The CDO may discontinue any collection for misuse of the authorization given. The Data Governance Commission shall review the recommendation and may rescind the authorization.

SECTION 1.02 PROCEDURE

Data collection requests are made using the Data Collection Request Form, to be filled out by the person initiating the data collection request. ADE employees are encouraged to consult the CDO and the data governance team to determine if suitable data is already collected by ADE prior to considering a new data collection request.

The request shall be reviewed and approved by the CDO and CPO. Upon approval, the requester shall consult with ADE IT architecture and IT operations to identify the most appropriate and cost effective method for collection.

The requests shall be evaluated by criteria including but not limited to:

1. The data element and applicable code values
2. The type of addition requested (a new element or new code value)

3. The method of collection
4. When the data will be collected and the frequency of collection
5. Any known system or other data element dependencies
6. The mandate, requirement, or other legal or statutory reference
7. A justification for the intended use, reason, or need for the data
8. An estimation of the impact of the collection, including any affected stakeholders, an estimate of the population, and any internal or external funding impact of the collection
9. A justification of the impact to the Arizona education system
10. Identified data owners and allowable data use and access

ARTICLE II. DATA CLASSIFICATION

SECTION 2.01 CONFIDENTIALITY

(A) STUDENT RECORDS

Student data shall remain confidential and may only be disclosed under very limited circumstances as permitted by federal law, state law and this policy. 20 U.S.C. 1232 g and A.R.S. § 15-1043. Student records are not public records under Arizona Law. A.R.S. § 15-1043. Any ADE report or data provided to any external party containing student records shall employ protections according to the level of access permitted.

The ADE has defined confidential student data to include any file containing data in which each record (or row in a table) pertains to an individual student, regardless of the contents of the fields included; or in which an aggregate count, percentage or other summary statistic of data, alone or in combination with other data, of a group of students is considered small enough, per this policy, to risk disclosure of a student's identity.

Except in the cases identified in this policy and in accordance with state and federal laws, datasets containing aggregate student data shall suppress results for small groups of students when associated with characteristics that would make it possible to identify a student. According to FERPA, confidential information includes "a list of personal characteristics or other information that would make it possible to identify the child with reasonable certainty." 34 CFR 99.3, 20 U.S.C. 1232(g).

(B) EDUCATOR RECORDS

The ADE has defined educator data to include all documents received by ADE for educator certification. Generally, the records received for educator certification are public except where a person has a privacy interest (for example, social security number, home address, home telephone). A.R.S. § 39-121.01. The post-secondary records provided for certification are confidential education records. 20 U.S.C. 1232(g). Evaluation performance classifications and evaluation reports are not a public record and may only be released under limited circumstances. A.R.S. § 15-537(I).

(C) EMPLOYMENT RECORDS

The ADE maintains personnel records for its employees. Public access is limited to these files except for name, date of employment and current and prior job title; current and prior salaries and dates; name of current or prior supervisors, in accordance with A.A.C. R2-5-105.

(D) PUBLIC RECORD

ADE is subject to Arizona's public records law. A.R.S. § 39-121.01(A)(1). Records are available for public inspection during business hours or upon request. A.R.S. § 39-121. Records that are not open for public inspection include records made confidential by statute and records involving privacy interests, as defined in this policy. ADE may also restrict access to records if it is the best interest of the state to do so where "inspection might lead to substantial and irreparable private or public harm." *Carlson v. Pima County*, 141 Ariz. 487, 491, 687 P.2d 1242, 1246 (1984).

SECTION 2.02 PROTECTION OF CONFIDENTIAL RECORDS IN AGREGATED REPORTS

ADE shall use approved methods to protect the confidentiality of records in any reports or release of aggregated data considered confidential, as defined in section 3.01 of this policy. At the discretion of the supervisor, ADE program areas may employ stricter methods of protecting confidentiality. Furthermore, datasets containing aggregate student data shall suppress results for small groups of students when associated with characteristics that would make it possible to identify a student except in the cases identified in this policy and in accordance with state and federal laws. A request for aggregate student data without cell suppression is considered to contain confidential data, and a request for restricted access to research data must be submitted, according to this Policy. Specific methods for redaction are available upon request to the Chief Data Officer.

ARTICLE III. ACCESS TO DATA

SECTION 3.01 OVERVIEW

ADE's policies and procedures for the processing of public records and data requests focuses staff efforts on the agency's mission and fulfills our responsibility to protect confidential data.

In order to maintain transparency of government and provide actionable information to parents, educators, and the community, ADE shall provide public datasets and reports that may be immediately downloaded and utilized. These publicly available data shall employ protections to maintain the confidentiality of student records and other data as appropriate.

ADE will respond timely to requests for public records or data sets if it is in a format currently maintained by ADE. ADE will only respond to requests for custom data sets from external parties as our resources allow. These types of requests will be processed in the order they are received and with the following prioritization.

1. Internal Requests by seniority of requester
2. Local education agencies or public schools within Arizona
3. All others requesters

All requests for public records or data must be made using the forms or tools available on ADE's website. Requests emailed to individual staff members shall be routed to this process and form for tracking purposes.

Data that is considered to be confidential will only be provided under limited circumstances as outline in this policy. This includes aggregate student or staff data without confidentiality protections, and individual-level student or staff data.

SECTION 3.02 FILES WITH CONFIDENTIAL DATA REMOVED

(A) POLICIES

ADE recognizes its legal obligation to respond to public records requests. Generally, all records necessary to provide an accurate accounting of official government-funded activities are presumed available for public inspection. ADE will respond timely to requests for public records or data sets if it is in a format currently maintained by ADE. ADE shall only fulfill public record requests for custom data extracts that require the allocation of staff resources to create as time permits; this type of request is not a public record as defined by Arizona law. A.R.S. 39-121.01 et seq.

All data provided under this section shall be reviewed and redacted to maintain the confidentiality of student records, educator records and other private information under state law. Student records are not public records under Arizona Law. A.R.S. § 15-1043.

(I) COMMERCIAL PURPOSE USE

Records are requested for a commercial purpose where the use of a public record is for:

1. Sale or resale or for the purpose of producing a document containing all or part of the copy for sale
2. Obtaining the names and addresses for solicitation or
3. Direct or indirect use of the public record for monetary gain.

The person who makes the request must provide a statement indicating the commercial purpose.

ADE may charge a fee to include: the cost of obtaining the document; reasonable fee for the cost of time, equipment and personnel to produce the record and the value of the reproduction on the commercial market as determine by ADE. ADE has determined that the charge for a commercial request of this nature is $.50 per email address.

(B) PROCEDURE

Public records request should be submitted via the request form available on ADE's website. For constituents who do not have access to the internet, ADE will process public records requests submitted by mail. ADE will make accommodations for persons with disabilities who submit requests. ADE cannot guarantee the timeliness of responses to requests that are not submitted through the procedures outlined in this policy.

Upon receipt of a request, ADE will determine if the request meets the definition of a public record, per this policy and Arizona law. ADE shall notify the requester of the determination within 10 business days of submission of the request. ADE shall also notify the requester if the request meets the definition of a request for commercial

purpose use. ADE shall notify the requester of the estimated date of response or work with the requester to identify a mutually acceptable timeline for producing rolling responses.

ADE will redact the data to maintain privacy. This applies to public records or aggregate data files as necessary. A request for aggregate student data without cell suppression is considered to contain confidential data, and a request form must be submitted, according to Section 4.03 of this Policy.

SECTION 3.03 REQUESTS FOR CONFIDENTIAL, UNREDACTED DATA

(A) POLICIES

Audit or Evaluation

This section applies to aggregate data without cell suppression and to individual-level student educational records or confidential Arizona educator data. Under federal law, ADE may respond to requests of this nature when the purpose of the request is linked to the evaluation or audit of a state or federally funded program. 34 CFR § 99.35. The requestor is made the authorized representative of the agency for the purpose of conducting the evaluation or audit. Requests of this nature require an ADE section sponsorship. A data protection agreement must be completed between the requestor and ADE for this type of request as described in Federal regulations. *Id*.

If the requestor does not have a sponsor, they can apply to conduct research under the restricted access research data process as outlined under section 4.03 (C). A requestor may seek to conduct a study for or on behalf of ADE to:

(1) Develop, validate or administer predictive tests;

(2) Administer student aid programs;

(3) Improve Instruction.

34 CFR § 99.31(a)(6)

ADE will consider such requests that meet the ADE criteria outlined in 4.03(C).

(B) SPONSORED DATA PROCEDURE

ADE may partner or contract with external entities to conduct its work and may share aggregate data without cell suppression and individual-level student or confidential staff data to conduct this work. The ADE sponsoring division must submit a request to be reviewed by the CDO and CPO. If approved, a data protection agreement as outlined by section 4.05 will be required. Upon execution of a Data Protection Agreement, ADE will provide the requested data via secure file delivery.

(C) RESTRICTED ACCESS RESEARCH DATA PROCEDURE

Student data shall remain confidential and may only be disclosed under very limited circumstances as permitted by federal law and this policy. ADE has discretion under federal law whether to allow restricted access to confidential student data based on exceptions in federal law (20 U.S.C. § 1232g and 34 CFR Part 99).

ADE shall designate a particular set of data to be determined at the discretion of the Chief Data Officer, to be used for restricted access research on site at ADE on a secure research computer. ADE shall make publicly available the list of data elements and years of data available for research and shall update this list no less than once annually or as changes occur. ADE will not update data extracts based on special requests, but will take requests into consideration for future enhancements of available restricted access data.

Any person or organization, including university faculty, independent researchers, and private and non-profit organizations, who wishes to use ADE's confidential data of any type, shall submit a research proposal to the ADE. All proposals and supporting documents sent to the ADE become public records. The ADE may refuse a research proposal request for student-level data and/or personally identifiable information for any reason. The authority to determine whether such requests are fulfilled is vested in the CPO and Chief Data Officer.

Once a requester has provided a complete packet of materials, the CPO and CDO will review the proposal and determine whether or not to grant the request. Incomplete packets will not be considered. Reviews will conducted within 10 business days of receipt of a complete proposal, based on availability of the CPO and CDO.

Upon approval of research proposal, ADE will notify the researcher(s) of the decision and the project shall be placed in a queue. The research team will be scheduled based on software needs and computer availability. ADE uses its discretion in prioritizing requests. ADE will make every attempt to provide access by the requested date, however ADE makes no guarantee that the data will be made available by the requested date. ADE will notify the requester within 10 business days if there is a change in schedule. Each individual being granted limited research access shall sign a Nondisclosure Agreement and the ADE End User Network Agreement, which shall include users who will be given access to conduct research, a list of data approved for use in the research project, and dates of user access.

The approved data shall be prepared and user accounts for approved research users shall be created. These user accounts shall be restricted as described above in this policy.

Using approved and available dataset, the researcher(s) will conduct analyses using software provided by ADE. Upon completion of analyses, the researcher(s) will save output files (e.g. sps file, or SAS output file) to the assigned drive, per instructions from ADE IT. ADE staff will review output for accuracy and appropriateness. If deemed inaccurate or inappropriate, the researcher(s) will modify the necessary analyses and resubmit results for review. Approved output will be delivered to the research(s) by ADE via email or secure file transfer.

Upon the conclusion of the research, the researcher(s) will submit any policy briefs, research papers, or other publications to ADE for review. Upon completion of the research or termination date in agreement, the user credentials and access will be terminated by ADE and the workspace files, Hdrive, or other files are archived and destroyed according to dates in the agreement.

(D) CRITERIA FOR EVALUATION OF SPONSORED AND EXTERNAL DATA REQUESTS

The CPO and CDO will use the following criteria for evaluation of internal and external data requests in addition to state and federal law.

1) Legality of the Project; Demonstration that the project complies with applicable laws and has a valid purpose
   a) Requests for research as part of a doctoral dissertation will not be considered
   b) Requests that will be used for marketing purposes will not be considered
2) Benefit to Arizona Students; Demonstration that the project will improve education, instruction, or other education-related issues specifically in Arizona. This shall be evaluated based on, but not limited to:
   a) An alignment with a topic or area of high priority for the ADE or the Superintendent of Public Instruction (e.g. a proposal identified by the Superintendent in the Arizona Kids Can't Afford to Wait)
   b) A unique or novel research question or contribution to the field of education, or testing an established theory or knowledge for its external validity to the Arizona education system
   c) A topic or approach with wide-reaching impact to the Arizona education system, or to a unique or underserved or under-researched population
3) Qualifications of Requestor; Demonstration that the researcher(s) has sufficient knowledge and experience to use the data appropriately, without drawing inaccurate conclusions. This shall be evaluated based on, but not limited to:
   a) Holding an advanced degree in education, social science measurement, psychometrics, or other similar field
   b) Experience in an applied or academic research setting using similar data
   c) The quality of training or demonstrated research abilities, including qualifications or status of the requester's organization
4) Quality of the work and research proposal; Demonstration that the project will employ formal, adopted and high quality research and statistical practices and research methodologies. This shall be evaluated based on, but not limited to:
   a) A high quality and appropriate analytical plan, that is directly relevant to and answerable with to the available data
   b) The uniqueness of the research question and contribution to the field of education

SECTION 3.04 INTERNAL STAFF DATA ACCESS

(A) USE OF DATA FOR INTERNAL RESEARCH OR REPORTS

An employee that wishes to be granted access to a specific application, or direct access to data stored on ADE systems or to gain internal access to data to use it for a purpose other than that for which the data was originally collected must obtain approval to do so.

If an employee does not normally have access to specific data for the employee's normal job duties, the employee must request access. The data use must be approved prior to the employee receiving access to or copies of the additional data. An employee that receives access to data under a data use request shall not disclose this data to any external entity.

(I) PROCESS

Employees shall submit a request to use data to the CDO and CPO for review. Employees shall provide a justification for the request that includes, but is not limited to: reason for the request, legal or rules citation, intended use of data, explanation of need for specific data elements. The CDO and CPO may consult with relevant data stewards to ascertain the appropriateness of the data usage or research question.

If the request is approved by the CDO and CPO, the ADE architecture review team will determine the best method to facilitate access to the needed data while ensuring the number of users granted direct access to ADE data stores is kept to a minimum. The database administrator of an ADE data source shall not grant direct access to any employee without an approved direct access request.

SECTION 3.05 DATA AGREEMENTS INITIATED BY ADE

All agreements in which the Department receives or shares data of any kind whether that be another state agency, non-profit organization or research group, must be signed by one of the Superintendent's designees and coordinated with the Legal division.

Authorized delegates currently include: Michael Bradley, Shari Zara and Ross Begnoche.

ARTICLE IV. VIOLATIONS OF THIS POLICY

ADE takes seriously its obligation to protect the personally identifiable information of students in Arizona public schools. ADE employees are expected to read this policy and participate in trainings on data privacy. ADE wants employees who may have inadvertently disclosed personally identifiable information to report such a disclosure IMMEDIATELY to his or her supervisor and ADE's Chief Privacy Officer. ADE will take immediate steps to ensure the information is recovered and/or destroyed by the recipient.

ARTICLE V. APPENDICIES

SECTION 5.01 APPENDIX A: REDACTION METHODS

SECTION 5.02 APPENDIX B: NON-DISCLOSURE AGREEMENT TEMPLATE FOR RESEARCHERS

State of Arizona

Department of Education

NON-DISCLOSURE AGREEMENT

The Arizona Department of Education ("ADE") enters into this Non-Disclosure Agreement ("Agreement") with **researcher** of **researcher's company** for **Name of study**.

A copy of the approved proposal will be kept on file at the ADE.

As an "agent" of the ADE you have access to confidential data. By signing below, Researcher acknowledges and agree:

1. That you have received a copy (or accessed online at www.azed.gov) of the Policies and Procedures of the ADE;

2. To abide by the terms of the ADE's policies and its subordinate process and procedures;

3. That you have completed formal Family Educational Rights and Privacy Act ("FERPA") training through either the ADE or another qualified institution;

4. To obtained the necessary human subject internal review board (IRB) approval (if required) by your institution or organization before assessing the Repository data at the ADE and supplied documentation;

5. To access and use the Repository data at the ADE only for authorized research;

6. That you will use the confidential data for only the purpose(s) of the study;

7. That you will not redisclose the results of your data analysis except to the co-author of your study without ADE's express written consent.

8. Not to attempt to identify individuals or publicly release confidential data;

9. That you understand that you must only access the Repository data at the ADE through your own credentials. Under no circumstance may a researcher log into the ADE under another researcher's account or allow another researcher to log in through their account;

10. Researchers must provide ADE with regular updates regarding the progress, changes, and extensions to the research hypotheses and personnel change for their research projects;

11. To ensure that all research conducted and all generated research products (including but not limited to papers, abstract, PowerPoint presentations, publication, etc.) using the Repository are compliant with FERPA, which explicitly means no information will be released that could identify individuals;

12. To never remove unapproved confidential information from the physical or electronic workspace of the ADE;

13. To ensure that all research output using the Repository data are compliant with the ADE Masking Guidelines & Techniques;

14. To never remove or publically release results or output that has not been approved for release from the physical or electronic workspace of the ADE;

15. To request the ADE review and approve all research products generated using confidential Repository data prior to any public release;

16. To report, as soon as possible, any known or suspected breach of confidentiality, including the removal or inappropriate sharing of data, to the Director or Database Administrator of the ADE;

17. That access to the ADE can be suspended based on any violation of this contract or risk of unauthorized disclosure of confidential information;

18. To grant permission for the manual and electronic collection and retention of security-related information, including but not limited to photographic or videotape images, of your attempts to access the facility and/or workstations; and

19. That you understand that the data files that you create for this project will be destroyed five years following the completion of the project, unless specific permission is granted for an extension by the ADE or another applicable state agency.

By signing this Agreement, **Researcher** agrees to comply with applicable ADE and FERPA regulations and requirements. By signing this Agreement, **Researcher** further acknowledges that s/he will use all information s/he reviews, observes, or receives only for the purposes of

the Partnership and that s/he will maintain all information s/he reviews or observes or receives in the strictest confidence

Researcher	**Shari Zara**
Date	Date

SECTION 5.03 APPENDIX C: ADDITIONAL SECURITY PRECAUTIONS AND GUIDELINES FOR DATA RESEARCHERS

ADE will be providing workstations for authorized researchers. Procedural guidelines for researchers to follow are available from the Data Governance group. This document lists the additional security measures applied to the accounts used by the researchers, as well as to the workstations they will be assigned to use.

A. ACCOUNT SECURITY MEASURES:

Each researcher will have an account created ahead of their anticipated use via the EUNA process.

1. Logon To Workstation set to ADE09014 and ADE08016 and fileh.prod.root server.
2. Access hours will only be permitted during working hours.
3. Account Expires set to 60 days – must be renewed every 60 days.
4. Each researcher's H: drive will be used to store all data by researchers.
5. No other file shares will be allowed.
6. No Internet access will be allowed.
7. No database access will be allowed.

B. WORKSTATIONS TO BE ASSIGNED:

Tag	**Brand/Model**	**Status**	**Special Software**
9014	HP Desktop	Stable	SPSS, STATA
8016	Dell Desktop Optiplex 7010	Stable	SPSS

C. WORKSTATION SECURITY MEASURES:

1. USB disabled
2. CDROM/DVD burner disabled
3. External IP ranges prohibited via FW rules preventing Internet traffic, inbound or outbound
4. Remote capability limited to Administrative/Support users.